AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: BB 6/17/2020

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of *(Briefly describe the property to be search* *Or identify the person by name and address)* INFORMATION ASSOCIATED WITH: Tyjross28@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY: Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043	Case No: M-20-280-STE

FILED
JUN 17 2020
CARMELITA REEDER SHINN, CLERK
U.S. DIST. COURT, WESTERN DIST. OKLA.
BY _____, DEPUTY

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following Property *(identify the person or describe property to be searched and give its location)*:

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized)*:

See Attachment B, which is attached and incorporated by reference

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252	Distribution of child pornography
18 U.S.C. § 2252A	Possession of child pornography

The application is based on these facts:

See attached Affidavit of Special Agent Ryder Burpo, HSI , which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of [No. of Days] days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Ryder J Burpo
Applicant's signature

RYDER BURPO
SPECIAL AGENT
HSI

Sworn to before me and signed in my presence.

Date: 6/17/20

Judge's signature

City and State: Oklahoma City, Oklahoma

SHON T. ERWIN, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Ryder Burpo, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises controlled by Google LLC, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC (Google) to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations (HSI) since June 2019, and am currently assigned to Oklahoma City, Oklahoma. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center Criminal Investigation Training Program and Homeland Security Investigations Special Agent Training, and everyday work relating to conducting these types of investigations. I have

received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have access to the institutional knowledge developed around this type of investigation by working with other experienced child exploitation criminal investigators. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252 and 2252A, and I am authorized by law to request a search warrant.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252 and 2252A have been committed by Tyler James ROSS using the email address tyjross28@gmail.com (the "SUBJECT ACCOUNT"), which is described in Attachment A of this affidavit. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

Initiation of Investigation and Overview of "Website M"

6. In March 2012, HSI Phoenix initiated an investigation into a password-protected, fee-based website, identified herein as "Website M,"[1] following an interview with a Website M user ("S1") in connection with a separate child exploitation investigation. S1 allowed HSI agents to assume S1's online identify on Website M and provided agents with S1's username and password.[2]

7. A user can only locate and access Website M if the user knows its current web address. Once the user enters the correct web address, a box appears that requires the user to enter a "user name" and "password." The user cannot access the site without first entering that information. Once the user enters a valid username and password, Website M's home page appears. The opening page depicts nude anime children (i.e., drawings, sketches or cartoons) lasciviously exhibiting their genitals. The term "Private Club" also appears on the home page.

8. After gaining access to Website M by using S1's username and login, HSI Phoenix agents determined that it advertises files of child pornography for purchase. Once logged in as a member, the user sees the names of folders available for purchase, which contain previews or samples of images contained in the folders. As of March 2012, the website advertised that it offered 600,000 images and 400 hours of video. Such images and videos are organized into

---

[1] Law enforcement knows the actual name of Website M. However, the investigation into users of Website M remains ongoing, and public disclosure of Website M's actual name would potentially alert its members to the investigation, likely provoking members to notify other members of the investigation, to flee, and/or to destroy evidence. Accordingly, to preserve the confidentiality and integrity of the ongoing investigation, the actual name and other identifying details of Website M remain undisclosed in this affidavit.

[2] S1 provided SAs with the web address for Website M and S1's login information to Website M but S1 has not provided sufficient information to law enforcement to understand how S1 originally obtained the web address or login information for Website M.

folders, the contents of which can be accessed after downloading them by purchasing a password. At all times relevant to this investigation, Website M hosted its content on a server physically located outside of the United States.

9. Throughout HSI's investigation, Website M has typically charged between $40 USD and $110 USD to purchase the password for encrypted archive files containing multiple images and/or videos of child pornography and child erotica. The majority of archive files cost $89 USD.[3] Once downloaded, the user can "decrypt" the selected archive file by entering in the purchased password to reveal multiple images and/or video files. Phoenix HSI Special Agents have made undercover purchases or accessed several archive files available for purchase revealing that most of the archive files contained between 500 and 2,000 image and/or video files, and the majority of which are child pornography.

10. HSI agents also found that Website M allows members to preview samples of the images/videos contained in an archive folder prior to purchase. HSI agents visited Website M and previewed more than 100 sample folders. Agents found that the majority of the images and videos found in the sample or preview folders depicted apparent minors, and many depicted what appeared to be pre-pubescent minors engaged in sexual activity with adults and/or posed in a sexually explicit manner.

11. Over the course of their investigation, which has involved previewing samples and then downloading multiple archive files via Website M, HSI agents have found that the sample

---

[3] A digital archive file is used to store multiple files within a single, compressed file, which can make it easier to store and transmit numerous files at the same time. File extensions associated with digital archive files include ".rar" and ".zip."

images and/or video screenshots corresponded to the full sets of image and video files contained in downloaded archive files.

12. After selecting an archive file for purchase, the member pays for its password via credit card. Website M then automatically sends an email to the member with the encryption password for the archive. The member must first download the archive file to a digital device and enter that password to decrypt and de-compress it.

Undercover Purchases Confirmed "Website M" Sells Child Exploitative Material

13. As noted above, HSI obtained membership information to Website M via a consensual takeover of S1's account. Between April 2014 and May 2017, HSI agents made multiple undercover purchases of archive files from Website M.

14. For example, in April 2014, HSI agents (posing as S1) successfully downloaded archive files from Website M. Review of the de-compressed image files, based upon an analysis of hash values, determined that the purchased files included video and image files from a series of images that the National Center for Missing and Exploited Children has identified and verified to depict a pre-pubescent minor child who appears to be less than ten years of age. Purchased files included the following: "180-2.AVI 9Yo Jenny licked by dog. 16min./with sound." The screenshot for this video depicts a nude, blindfolded, prepubescent female who appears to be less than ten years of age lying on her back while a dog licks her genitals. Over twenty additional pictures from the same series were included, such as an image of the same nude prepubescent female performing fellatio on a dog.

Financial Records Linked to Website M

15. On May 26, 2017, an HSI agent, working in an undercover capacity, purchased an archive file from Website M titled "SIBERIAN MOUSE #36." This file was selected because it

was listed on the opening page as being newly added (as of January 2017) and agents verified the images within the sample folder contained images depicting apparent minors engaged in sexually explicit conduct. When the HSI agent purchased the "SIBERIAN MOUSE #36" file, the agent received a confirmation email from "TheScript Support" through a payment processor based in the United States that stated, "Your order is currently being processed."

16. HSI agents investigated the link between the US-based payment processor and Website M. HSI agents identified the U.S. company as both a payment processor and online business management tool used by Website M.

17. On July 28, 2017, a U.S. magistrate judge in the United States District Court for the District of Arizona issued a search warrant for the electronic data in the possession of the U.S. payment processor related to their business transactions with and on behalf of Website M.

18. On August 11, 2017, the U.S. payment processor provided several spreadsheets in compliance with the search warrant. One of the spreadsheets listed all the transactions the company processed on behalf of Website M. This list included over 1,000 purchases made to Website M.

Identifying Tyler James ROSS as a Purchaser of Child Exploitative Material from Website M

19. In September 2017, HSI analyzed the U.S. payment processor records and identified individuals who made multiple purchases from Website M.

20. The U.S. payment processor records indicate that Tyler ROSS made approximately three (3) purchases from Website M between March 4, 2016 and October 3, 2016.

21. According to the U.S. payment processor records, the email address to which it sent the auto-generated receipts and passwords for purchases made by ROSS on Website M was Tyjross28@gmail.com (the "SUSPECT EMAIL ADDRESS").

22. In response to a summons, the U.S. payment processor, provided the following subscriber information associated with the two accounts associated with the Tyler ROSS purchaser:

First Name: Tyler

Last Name: ROSS

Email: Tyjross28@gmail.com

AKA: Joe Smith

Address: 959 Cumberland Mansion, Yukon, Oklahoma 73099

555 SW 9th Street, Oklahoma City, Oklahoma 73102

Mobile Telephone Numbers: (405) 819-4922; (559) 228-8228

Frequent IP Addresses: 68.229.195.45 , 70.215.215.215 , 70.215.195.73 , and 70.215.195.158

Internet Subscriber Address: 2721 Lakeside Drive, Oklahoma City, Oklahoma 73120

Internet Subscriber Name: Katherine Cunningham

Address: 2721 Lakeside Drive, Oklahoma City, Oklahoma

House Owner: Katherine Cunningham

23. In May 2017, the United States Department of Justice, through a letters rogatory, formally requested assistance from the host nation of one of the Website M content servers. HSI obtained records and content from the Website M content server.

24. On December 21, 2017, a U.S. magistrate judge in the United States District Court for the District of Arizona issued a search and seizure warrant for the hard drive containing the content of the Website M server. In March 2018, through a supplemental letters rogatory request, HSI obtained an updated imaged copy of the server used to host Website M. A computer forensic

agent verified that the server contained the content, specifically child pornography and child exploitive material for Website M, specifically the folders purchased by ROSS. I reviewed files indicated by the purchase records to have been purchased by ROSS, including each file from ROSS' most recent purchases from October 3, 2016, and I found that the files contain images depicting minors engaging in sexually explicit conduct.

25. The forensic agent also located member usernames and emails. He was able to determine when members logged onto the website and what IP addresses were used by the member. Website M content server records indicate that username "tyjross28" was found on the server and that tyjross28 logged onto Website M over eighty five (85) times, including October 3, 2016 from IP address 68.229.195.45. Open source database checks revealed that IP address 68.229.195.45 has a geolocation in Oklahoma.

26. In response to a summons, Cox Communications, Inc. (Cox) provided subscriber information that indicates that IP 68.229.195.45 is assigned to Katherine Cunningham residing at 2721 Lakeside Drive, Oklahoma City, Oklahoma 73120.

27. The U.S. payment processor records indicate that on or about March 5, 2016 ROSS purchased a password for an archive file with the billing code "AJAX SCRIPT 26." Records from the Website M content server indicate that on March 5, 2016 at approximately 16:13 hours (MDT) tyjross28 logged into Website M from IP address 68.22.195.45.

28. In December 2018, HSI Oklahoma City received information from the HSI Phoenix office indicating that the Internet Protocol (IP) address 68.229.195.45, was utilized, by a subject using the email address of Tyjross28@gmail.com, to purchase child exploitative material from Website M. On August 1, 2019, HSI Oklahoma City, served Cox Communications, Inc. (Cox) with a Department of Homeland Security Summons, requesting the subscriber identity for the

person who was assigned the IP address 68.229.195.45. On September 01, 2019, I received a response from a Subpoena Specialist for Cox, indicating that the IP address (68.229.195.45) listed in the HSI Summons, returned to Katherine Cunningham at 2721 Lakeside Drive, Oklahoma City, Oklahoma 73120.

29. According to a check of open source databases Tyler James ROSS resided at 959 Cumberland Mansion Road, Yukon, Oklahoma 73099 until October 2018. At that point in time ROSS appears to move to 218 28th Street Northwest, Oklahoma City, Oklahoma 73103 from October 2018 to February 2019. Approximately March 2019 is when ROSS is listed as residing at 2721 Lakeside Drive, Oklahoma City, Oklahoma 73120. ROSS' recent driver's license renewal of May 2020 currently lists 2721 Lakeside Drive, Oklahoma City, Oklahoma 73120 as his current residence.

30. In July of 2019, Homeland Security Investigations (HSI) Oklahoma City Office received a tip from Oklahoma State Bureau of Investigation on behalf of the National Center for Missing and Exploited Children (NCMEC). This tip was about the possession, manufacture, and distribution of images of child pornography in the Google Photos account associated with tyross28@gmail.com. This email account, tyjross28@gmail.com is registered to Tyler Ross (ROSS). There were multiple instances from September 2018 through June 2019 of uploads containing child exploitative material into the Google Photos infrastructure. There was a total of fifty-three (53) files reported to Google and forwarded to NCMEC. Based on the cyber tipline report received, a NCMEC staff member reviewed multiple files associated with the Google photos account of tyjross28@gmail.com. A review of the reported files found there were multiple instances of child pornography.

31. The Internet Protocol (IP) address of 68.229.195.45 was recorded as having multiple log in records to the Google Photos account of tyjross28@gmail.com. This IP address, 68.229.195.45, was previously found to be registered to Katherine Cunningham at 2721 Lakeside Drive, Oklahoma City, Oklahoma 73120.

Evidence That ROSS Downloaded Child Exploitive Material from Website M

32. Based upon the U.S. payment processor records, HSI generated the following list of purchases ROSS made via the U.S. payment processor from Website M along with identifying information linked to each purchase.

Date	File Purchased	First Name	Last Name	Phone	Email	Address
03/04/2016	AJAX 19	Tyler	Ross	(405) 819-4922	Tyjross28@gmail.com	959 Cumberland Mansion, Yukon, OK 73099
03/22/2016	AJAX 24	Joe	Smith	(559) 228-8228	Tyjross28@gmail.com	
03/05/2016	AJAX 26	Tyler	Ross	(405) 819-4922	Tyjross28@gmail.com	959 Cumberland Mansion, Yukon, OK 73099

33. After obtaining ROSS' purchase history from the U.S. payment processor, an HSI Phoenix agent, in an undercover capacity, viewed "samples" from each file titled in the above purchase records. The previews were recorded using screen capture software available to law enforcement. I have reviewed previews from some of the files referenced in the table above that consist of images depicting minors engaging in sexually explicit conduct.

34. Based on undercover purchases from Website M, HSI agents determined that the only way someone can view the full content of the archive file selected appears to be to: 1) download the archive file from the website; and 2) enter the password provided by the website,

via email, after payment is verified. There does not appear to be any way to view the full content of folders within the site itself, even with a purchased password.

35. Based on undercover purchases from Website M, the investigation, and my training and experience, it appears that Website M generates a billing name for each archived file available for purchase that corresponds with the name of a commonly purchased "script," in order to disguise the actual contents of the file purchased from the payment processor or anyone else who has access to the billing statement. Note that, in the chart above, almost all of the purchases contain a title that includes the term "script." A script is computer code or software that makes a computer run smoother and faster. Some examples are "PERL SCRIPT," "RUBY SCRIPT," and "PHP SCRIPT." Website M named each of the archive files it sells so that it would appear as if its Members purchased scripts instead of child pornography. The investigation further revealed that Website M registered its business with the U.S. payment processor under the name "The Scripts" in order to appear as a legitimate company.

36. On March 22, 2016, ROSS purchased a password for an archive file with the billing code "AJAX SCRIPT 24". HSI agents located an archive file on Website M titled "AJAX SCRIPT 24". When HSI agents clicked on this archive file on Website M, the website provided the following prompt at the bottom of the webpage "BUY NOW PASSWORD FOR "AJAX SCRIPT 24" . When HSI agents clicked on this prompt, the webpage displayed an option to buy "AJAX SCRIPT 24" with an "Immediate License Code sent by Email."

37. I reviewed a screen capture of the "samples" viewed from "AJAX SCRIPT 24". I observed several "sample photos," including the image file described below:

38. "AJAX SCRIPT 24" contains a file folder labeled 24. Within the file folder labeled 24 there are approximately twelve (12) file folders labeled with female names. In the file folder

labeled "Angel" there are approximately 51 images. In the file folder labeled "Angel" there is an image labeled "Mvc-008s-for_me.jpeg". This image depicts a Caucasian pre-pubescent female with one of her hands grasping a Caucasian adult male's erect penis. The child victim's mouth was on the adult male's penis as the female looks upward.

39. As a second example on March 5, 2016, ROSS purchased an archive file with the billing code "AJAX SCRIPT 26." HSI agents located an archive on Website M titled "AJAX SCRIPT 26." When agents clicked on this archive file on Website M, the webpage displayed an option to buy "AJAX SCRIPT 26." with an "Immediate License Code sent by Email."

40. I reviewed the screen capture of the "samples" viewed from "AJAX SCRIPT 26." file. I observed multiple "sample photos," including the image file described below.

41. "AJAX SCRIPT 26" contains 27 file folders labeled various things. One of those file folders is labeled "4yo Melinda." Within the file folder labeled "4yo Melinda" there are 106 images. One of the images is labeled "melinda44.jpeg." This image depicts a Caucasian pre-pubescent, under 6 years old, female with the focal point of the photo being on her genital area. The child's genitals lacked pubescent hair development. An adult Caucasian male was penetrating the anus of the child with his erect penis.

42. On September 7, 2018, an HSI intelligence research specialist sent a preservation request to Google requesting that the contents of the SUBJECT ACCOUNTS be preserved. On June 2, 2020, I sent another preservation request to Google requesting that the contents of the SUBJECT ACCOUNTS be preserved.

BACKGROUND CONCERNING EMAIL

43. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows

subscribers to obtain email accounts at the domain name Gmail.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

44. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

45. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

46. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

47. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

48. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the

information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

49. In my training and experience, I have learned that an email that is sent to a Google subscriber is stored in the subscriber's email mailbox on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on

Google servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

50. In my training and experience, I have learned that Google in addition to providing email services provides other services associated with the email account such as photo storing capabilities, known as Google Photos, online file hosting and synchronization services, known as Google Drive, that are available to the public. While users may delete photos or files off their account storage, it may still be available in Google's servers for a certain period of time.

51. Google provides fifteen (15) gigabytes of free storage to be shared across all Google services. This storage includes Google email, Google photos, and Google drive.

CONCLUSION

52. Based on the forgoing, I request that the Court issue the proposed search warrant. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Ryder Burpo
Special Agent
HSI Oklahoma City

Subscribed and sworn to before me on June 17, 2020

HONORABLE SHON T. ERWIN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with tyjross28@gmail.com that is stored at the premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f) on September 7, 2018 and June 3, 2020, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the accounts from March 4, 2016 to June 2, 2020, including stored or preserved copies of emails sent to and from the accounts, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the accounts, including contacts with support services and records of actions taken. The Provider is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.

f. Notwithstanding Title 18, United States Code, Section 2252A, Google may disclose responsive data, if any, by delivering encrypted files through Google's Law Enforcement Request System (LERS) or via a mailing/shipping service provider, such as FedEx, United Parcel Service (UPS), or the United States Postal Service.

Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of title 18, U.S.C., §§ 2252 and 2252A, those violations involving Tyler ROSS, tyjross28@gmail.com, and occurring after March 4, 2016, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) All images of child pornography and child erotica and written communications regarding child pornography and child erotica and all communications with minors. Any evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(b) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(c) The identity of the person(s) who created or used the email account, including records that help reveal the whereabouts of such person(s).